Cisco Certified Network Associate (CCNA) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. To check that interfaces are not set to passive on an OSPFv3 network, which command should be utilized?

A. #show ipv6 ospf interface

B. #show ipv6 routing status

C. #show ipv6 link-status

D. #show ipv6 ospf database

2. Which protocol operates on UDP port 53?

A. FTP

B. DNS

C. TFTP

D. SNMP

3. What are the two basic types of VPNs?

A. Public and Private

B. Intranet and Extranet

C. Site-to-Site and Remote Access

D. Local and Wide Area

4. Which command can be used to debug OSPF Hello packets?

A. #debug ip ospf packet

B. #show ip ospf interface

C. #debug ip ospf hello

D. #show ip ospf

5. In SNMPv3, which feature enhances security compared to SNMPv2?

A. Community strings

B. Encryption

C. Inform protocol

D. Trap messages

6. Which of the following approaches is NOT used when migrating from an IPv4 addressing scheme to an IPv6 scheme?

- **A. Dual-stack routing**
- **B. Configure IPv4 tunnels between IPv6 islands**
- **C. Port forwarding**
- **D. Proxying and translation to translate IPv6 packets into IPv4 packets**

7. What does the PPP LCP function called Link-Quality Monitoring (LQM) do?

- **A. Optimizes data flow**
- **B. Monitors router bandwidth usage**
- **C. Disables an interface exceeding error threshold**
- **D. Establishes connections between protocols**

8. What are the two configurations needed to set up EIGRP for IPv4?

- **A. router eigrp AS NUMBER; network NETWORK TO BE ADVERTISED**
- **B. router eigrp AS NUMBER; passive-interface INTERFACE NUMBER**
- **C. maximum-paths NUMBER; metric maximum-hops NUMBER**
- **D. network NETWORK TO BE ADVERTISED; no-auto-summary**

9. Which type of connection utilizes the command 'no shutdown'?

- **A. Ethernet connection**
- **B. Serial connection**
- **C. Wireless connection**
- **D. Fiber connection**

10. What is the command to configure a specific OSPF network type on an interface?

- **A. (config-if)#ip ospf type NETWORK_TYPE**
- **B. (config-if)#ip ospf network NETWORK TYPE**
- **C. (config-if)#ospf network NETWORK TYPE**
- **D. (config-if)#set ospf network NETWORK TYPE**

Answers

1. A
2. B
3. C
4. C
5. B
6. C
7. C
8. A
9. B
10. B

Explanations

1. To check that interfaces are not set to passive on an OSPFv3 network, which command should be utilized?

A. #show ipv6 ospf interface

B. #show ipv6 routing status

C. #show ipv6 link-status

D. #show ipv6 ospf database

The selected command to check that interfaces are not set to passive on an OSPFv3 network is indeed the correct choice. This command provides detailed information about each interface that is participating in the OSPFv3 process, including the operational status of those interfaces. Specifically, it displays whether an interface is set to passive or active for OSPFv3, which is crucial for ensuring that OSPFv3 is functioning properly and that routing updates can be exchanged between routers on the network. Other options may provide useful information but do not specifically address the requirement of checking for the passive status of interfaces in an OSPFv3 configuration. The routing status command typically gives a summary of the routing table, the link-status command relates to the physical layer connectivity, and the OSPF database command is oriented towards understanding the routing information database's content rather than the operational state of the interfaces. Thus, to directly check for passive interfaces, the first command is the most appropriate choice.

2. Which protocol operates on UDP port 53?

A. FTP

B. DNS

C. TFTP

D. SNMP

The protocol that operates on UDP port 53 is the Domain Name System (DNS). DNS is essential for translating human-readable domain names, like www.example.com, into their corresponding IP addresses, which are required for locating and accessing resources on the internet. It utilizes UDP for most of its queries due to the nature of the requests, which typically involve small amounts of data and require quick responses. Using UDP allows for faster communications since it does not establish a connection before data transmission, making it suitable for the rapid query-response nature of DNS. If a query or response is lost, the application can simply resend the request without needing a complicated handshake process. While some protocols may also use port 53, such as DNS over TCP for larger responses or zone transfers, the primary and most recognized use of UDP port 53 is for DNS service. Other protocols, such as FTP, TFTP, and SNMP, operate on different ports and serve different purposes in the networking environment; for example, FTP uses ports 21 and 20, TFTP uses port 69, and SNMP uses port 161. This context clarifies why DNS is the correct answer for this question.

3. What are the two basic types of VPNs?

A. Public and Private

B. Intranet and Extranet

C. Site-to-Site and Remote Access

D. Local and Wide Area

The two basic types of Virtual Private Networks (VPNs) are indeed Site-to-Site and Remote Access. Understanding these two categories is crucial for network design and implementation. Site-to-Site VPNs create a secure connection between two or more networks (typically separate office locations) over the internet. This type of VPN allows for secure communication over an untrusted network as if the connected networks were part of the same local area network (LAN). It is commonly used by organizations to connect branch offices to a central office securely. Remote Access VPNs, on the other hand, allow individual users to connect to a network securely from remote locations. This is particularly useful for employees who need access to the corporate network while working from home or while traveling. Remote Access VPNs authenticate users and encrypt the data transmitted over the connection, providing a secure channel for individual users. Both types ensure that data remains secure and private even when traversing potentially insecure networks, fulfilling the purpose of a VPN. Understanding these distinctions helps in selecting the appropriate type of VPN based on the organization's requirements and use cases.

4. Which command can be used to debug OSPF Hello packets?

A. #debug ip ospf packet

B. #show ip ospf interface

C. #debug ip ospf hello

D. #show ip ospf

The command that can be used to debug OSPF Hello packets is indeed the one that specifically targets the Hello packets used within the OSPF protocol. This command enables real-time monitoring of OSPF Hello packets, which are essential for establishing and maintaining neighbor relationships between routers within an OSPF network. Using this command allows network engineers to observe the details of the Hello packets being sent and received, including the interval between Hello packets and the settings that affect OSPF neighbor discovery. This is especially useful for troubleshooting issues related to OSPF adjacencies or neighbor formation. The other options, while related to OSPF, do not effectively allow for the same level of granularity in debugging Hello packets. For instance, the command that lists OSPF interfaces provides configuration and status information about OSPF-enabled interfaces but does not offer packet-level debugging. The command designed for general OSPF debugging will cover all OSPF packets, not just the Hello packets, which may produce more output than is relevant for a specific issue related to neighbor formation. By focusing on the OSPF Hello packets, network professionals can streamline their troubleshooting efforts, making this command particularly valuable in diagnosing connectivity issues in OSPF deployments.

5. In SNMPv3, which feature enhances security compared to SNMPv2?

A. Community strings

B. Encryption

C. Inform protocol

D. Trap messages

Encryption is a key feature that enhances security in SNMPv3 compared to SNMPv2. In SNMPv2, communication between devices relies primarily on community strings for authentication, which are essentially plaintext passwords. This method lacks robust security as community strings can easily be intercepted. In contrast, SNMPv3 incorporates a more comprehensive security model that includes options for encryption of the SNMP messages themselves. This encryption secures the data being transmitted, making it significantly more difficult for unauthorized users to capture and read sensitive information, thus ensuring the confidentiality and integrity of data over the network. While the other options do describe elements of communication in SNMP, they do not contribute to security enhancements to the same extent as encryption does. For instance, community strings are a method of basic authentication but are not secure, as they can be easily compromised. The Inform protocol, on the other hand, is used for reliable message delivery but does not directly enhance security. Trap messages are notifications sent from an SNMP agent to a manager and likewise do not address security issues present in earlier versions.

6. Which of the following approaches is NOT used when migrating from an IPv4 addressing scheme to an IPv6 scheme?

A. Dual-stack routing

B. Configure IPv4 tunnels between IPv6 islands

C. Port forwarding

D. Proxying and translation to translate IPv6 packets into IPv4 packets

When migrating from an IPv4 addressing scheme to an IPv6 scheme, various approaches facilitate the transition while ensuring that both protocols can coexist and communicate as needed. The correct answer highlights a method not typically associated with this migration process. Dual-stack routing allows a network to run both IPv4 and IPv6 simultaneously, enabling devices to communicate using either protocol without disrupting existing services. This approach is essential during the transition as it accommodates both addressing schemes. Configuring IPv4 tunnels between IPv6 islands is another common method where encapsulation techniques create paths for IPv6 packets to travel over an IPv4 infrastructure. This supports interoperability across networks that have not yet fully transitioned to IPv6. Proxying and translation involve mechanisms like NAT64, which enable IPv6 devices to communicate with IPv4 resources by translating and proxying the packets. This method is instrumental in helping the old and new addressing schemes interact. In contrast, port forwarding is not a recognized approach specifically employed during the migration from IPv4 to IPv6. It is primarily a technique used in network address translation to redirect traffic from one IP address and port combination to another, typically within the same IPv4 address space. While port forwarding has its merits in IPv4 environments, it doesn't directly aid in the transition to IPv

7. What does the PPP LCP function called Link-Quality Monitoring (LQM) do?

A. Optimizes data flow

B. Monitors router bandwidth usage

C. Disables an interface exceeding error threshold

D. Establishes connections between protocols

The Link-Quality Monitoring (LQM) function within Point-to-Point Protocol (PPP) is designed to assess the quality of the link between two endpoints. Its primary role is to track error rates and link performance, ensuring that the communication link remains reliable. If the LQM detects that the error rate surpasses a defined threshold, it responds by taking action to maintain network stability and performance, specifically by disabling the interface. This minimizes the impact of a poor-quality link on the overall network operations, thereby enabling the network devices to avoid sending data over a failing link. By using LQM, network administrators can maintain a healthy network environment, as LQM helps proactively manage connections based on the detected quality of the link. This is crucial for maintaining efficient and reliable data transmissions in a network. Thus, the action of disabling an interface that exceeds the error threshold accurately captures the intent and function of LQM within PPP.

8. What are the two configurations needed to set up EIGRP for IPv4?

A. router eigrp AS NUMBER; network NETWORK TO BE ADVERTISED

B. router eigrp AS NUMBER; passive-interface INTERFACE NUMBER

C. maximum-paths NUMBER; metric maximum-hops NUMBER

D. network NETWORK TO BE ADVERTISED; no-auto-summary

To effectively set up EIGRP (Enhanced Interior Gateway Routing Protocol) for IPv4, it is essential to configure both the EIGRP process and specify which networks will be included in the routing process. The first part of the correct answer involves initiating the EIGRP routing process with the command `router eigrp AS NUMBER`, where "AS" stands for Autonomous System. This establishes the EIGRP instance on the router and allows the router to participate in routing within the specified autonomous system. The second part involves using the `network NETWORK TO BE ADVERTISED` command, which guides the router on which interfaces should participate in the EIGRP process. This command will match the IP addresses configured on the router's interfaces to the network specified and ensure those networks are advertised to other EIGRP neighbors. In summary, both the initiation of the EIGRP process and the specific identification of networks to be advertised are crucial for establishing a functioning EIGRP environment. Thus, this choice captures the fundamental steps necessary for successfully configuring EIGRP for IPv4.

9. Which type of connection utilizes the command 'no shutdown'?

A. Ethernet connection

B. Serial connection

C. Wireless connection

D. Fiber connection

The command 'no shutdown' is commonly used in networking to enable an interface on a router or switch. When this command is applied to a serial connection, it serves to activate that specific interface, allowing for data transmission. By default, many interfaces on Cisco devices are administratively shut down, meaning they will not transmit or receive data until explicitly enabled using the 'no shutdown' command. In the context of Ethernet, wireless, and fiber connections, the command is still applicable, but its most notable use and frequent association in practice is with serial connections, especially in the context of point-to-point communications found in many routing scenarios. Understanding how and when to use 'no shutdown' is crucial for configuring interfaces properly across various types of connections.

10. What is the command to configure a specific OSPF network type on an interface?

A. (config-if)#ip ospf type NETWORK_TYPE

B. (config-if)#ip ospf network NETWORK TYPE

C. (config-if)#ospf network NETWORK TYPE

D. (config-if)#set ospf network NETWORK TYPE

The command to configure a specific OSPF network type on an interface is correctly represented by the option that uses the syntax `(config-if)#ip ospf network NETWORK TYPE`. This command is essential in OSPF (Open Shortest Path First) configurations because it defines how the OSPF protocol recognizes and operates within the specified network segment. When you apply this command in interface configuration mode, you can specify the network type, which can greatly influence how OSPF operates in terms of neighbor relationships and routing table updates. The supported network types include point-to-point, broadcast, non-broadcast multi-access (NBMA), and others. Each type serves a different purpose, and the assigned type can impact OSPF's behavior in the network. For instance, a point-to-point link is treated differently compared to a broadcast network, leading to different methods in establishing adjacencies and exchanging routing information. The other options are not valid commands recognized by Cisco IOS for configuring OSPF network types on interfaces. They either use incorrect syntax or do not conform to the command structure defined by Cisco's operating system. Understanding the correct command is crucial for effective OSPF configuration and ensures that the network operates smoothly by establishing appropriate protocols for routing within varying network